PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Rhoads

Application No. 09/198,022

Filed: November 23, 1998

For: SECURITY DOCUMENT WITH
       STEGANOGRAPHICALLY-
       ENCODED AUTHENTICATION
       DATA

Examiner: Dr. B. Tadayon

Date: June 26, 2000

Art Unit 2721

RECEIVED

ᴵJUL 0 7 2000

GROUP 2700

APPEAL BRIEF

BOX AF
ASSISTANT COMMISSIONER FOR PATENTS
Washington, DC 20231

Sir:

This brief is in furtherance of the Notice of Appeal filed May 1, 2000. The fee required
under 37 CFR 1.17(f) is to be charged to Deposit Account 50-1071 (see transmittal letter).

I. REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventor recorded at Reel 7652, Frames 0225--227.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-17 are finally rejected. No claim stands allowed.

IV. STATUS OF AMENDMENTS

An Information Disclosure Statement is submitted herewith. All other papers have been entered.

V. SUMMARY OF THE INVENTION

The invention relates to passports, drivers' licenses, and other security documents, and more particularly relates to such documents having graphics that are steganographically encoded with plural bits of digital data so as to facilitate document authentication.

According to one aspect of the invention, such a document includes a graphic (e.g., a passport photo) into which plural bits of data are steganographically encoded.[1] These bits are used – in conjunction with text printed on the document – to verify authenticity of the document. The plural bit data can represent, for example, the passport number or bearer name of the passport.[2] If the document is later altered by photo-swapping, the swapped-in photo will not

---

[1] Specification, page 2, lines 4-5.
[2] Specification, page 10, lines 25-26.

have the same digital data. (If the photo is taken from another passport, it may have embedded data representing the bearer name or passport number of the passport from which it was taken. If the photo is taken from another source it will likely have no embedded data.) When such a doctored passport is analyzed, if the digital data recovered from the photo does not correspond to the text printed on the document, the passport is known to be a forgery.

In accordance with another aspect of the invention, a photo ID document includes a photo portraying an individual. Steganographically encoded within the photograph is multi-bit data. This steganographic encoding does not visibly interrupt the photograph, but serves to add noise thereto.[3] This noise is not perceptible as a representation of the multi-bit information except by computer analysis.[4] Accordingly, the encoded photograph appears to convey only an image of the individual to human viewers thereof.[5]

All of the claims require "steganographic" encoding. Steganography, as understood by artisans in the field, means *to hide secret information in some other data without leaving any apparent evidence of data alteration.*[6]

VI.   ISSUE

Did the Office err in making a nonstatutory obviousness-type double patenting rejection of all claims over applicant's patent 5,850,481?

Did the Office err in rejecting claims 1-6, 8-13, and 15-16 as anticipated by Nathans 4,972,476?

---

[3]   Specification, page 2, lines 4-6, 14-16.
[4]   Specification, page 2, lines 6-7.
[5]   Specification, page 2, lines 7-8.
[6]   Of record in this application (submitted January 18, 2000), and supporting such common understanding, is a paper from a recognized scientific journal: Kawaguchi, *Principles and Applications of BPCS-Steganography*, Proceedings of the SPIE, Vol. 3528, pp. 464-73, Nov 2-4, 1998.

VII. GROUPING OF CLAIMS

Claims 2, 3 and 16 stand or fall with claim 1.

Claims 9, 10 and 15 stand or fall with claim 8.

Each of the other claims is separately patentable, as detailed below.

VIII. ARGUMENT

1. Non-Statutory, Obviousness-Type, Double-Patenting Rejection over 5,850,581

The Final Action included two nonstatutory obviousness-type double patenting rejections
– one premised on 5,841,886, and the other premised on 5,850,481.

In an Amendment After Final mailed January 18, 2000, applicant submitted a Terminal
Disclaimer over the '886 patent, but declined to submit such a disclaimer as to the '481 patent
since applicant believes no such disclaimer was warranted.

The Final Action alleged that the claims of the '481 patent are not patentably distinct
from the pending claims. The remarks supporting this rejection read, in their totality, "see claim
number 1 of the parent cases, compared to claim 1 of the current case."

As an initial point, applicant respectfully submits that the quoted remarks do not establish
a prima facie case. The burden to establish non-patentability rests with the Examiner. This
burden should not be shifted to applicant by a conclusory statement with no factual details or
analysis.

On the merits, the rejection is ill-founded. Taking the claims cited by the Examiner,
claim 1 of the '481 patent is drawn to a paper medium with embedded data formed by
modulating two signals to produce a third, and shaping the micro-topology of the paper medium
(i.e. texturing) in accordance with the third signal.

Pending claim 1 does not require modulating two signals to produce a third. Nor does it
require shaping the micro-topology of a paper medium.

Conversely, issued claim 1 of the '481 patent does not require a security document. It does not require text printed on the document. It does not require a graphic on the document. The two claims are presented below for comparison:

Pending Claim 1	Issued Claim 1 of '481
1. A security document comprising: a substrate; text printed on the substrate; a graphic carried by the substrate, the graphic conveying a visual impression to human viewers thereof; the graphic additionally being steganographically encoded to secretly convey plural bits of digital data recoverable by computer analysis of said graphic	1. A paper medium having steganographically encoded data stored therein, the steganographically encoded data being produced in accordance with the following method: providing first and second signals; modulating the first signal with the second to produce a third signal, wherein the second signal cannot be discerned from the third signal without the first signal; shaping the surface micro-topology of the paper medium in accordance with the third signal.

Applicant respectfully submits that these two claims are patentably distinct. As such, the nonstatutory, obviousness-type double patenting rejection should be reversed.

2.   Anticipation Rejection of Claims 1-6, 8-13, and 15-16 Over Nathans 4,972,476

Like certain applications of the documents claimed by applicant, Nathans' addresses the problem of photo-swapping in identification documents, e.g., in identification badges used at military facilities.[7] However, Nathans rests on totally different principles.

Nathans' photo ID document is printed with a *scrambled* facial image.[8] Not all of the image needs to be scrambled,[9] but enough to be conspicuous to a document inspector.[10]

The scrambling is done with an algorithm employing a PIN code or other data known to the bearer (e.g., the last three digits of the bearer's social security number).[11] When the card is presented to a document inspector, the scrambled photograph is digitally scanned and displayed on a verifier terminal. The bearer then enters the PIN code on a keypad.[12] The terminal applies an inverse-scrambling procedure based on the PIN code.[13] If the user has entered the correct PIN code, the photograph is correctly unscrambled.[14] The inspector can then compare the unscrambled picture on the terminal with the person and, if they match, authorize entry to restricted premises. If an incorrect code is entered, the photograph does not unscramble.[15]

As noted, each of the pending claims requires *steganographic* encoding of a graphic or photograph on a document. As noted, steganography refers to the hiding of secret information in some other data *without leaving any apparent evidence of data alteration.*

Nathans' image scrambling is not steganography. While the essence of steganography is inconspicuousness, Nathans relies on the opposite attribute: *conspicuousness.* "If the image on the monitor is not fully descrambled, the guard is alerted."[16] Rather than teaching applicant's claimed approach, Nathans teaches the opposite.

Each of the Section 102 rejections should be reversed for this reason.

---

[7]   Nathans, col. 1, line 11.
[8]   The title of Nathan's patent is *Counterfeit Proof ID Card Having a Scrambled Facial* Image.
[9]   Nathans, col. 2, lines 42-46.
[10]   Nathans, col. 4, lines 7-11; Fig. 2, e.g., scrambling "a stripe extending between the forehead area 14 and the chin area."
[11]   Nathans, col. 2, lines 65-66.
[12]   Nathans, col. 4, lines 47-50.
[13]   Nathans, col. 4, lines 50-54.
[14]   Nathans, col. 4, lines 55-58.
[15]   Nathans, col. 5, lines 5-9
[16]   Nathans, col. 5, lines 19-20.

The Final Action includes a variety of citations to Nathans. Except for claims 2, 3, 9, and 10, applicant respectfully submits that none of these citations supports the features for which they are offered.

Claim 1

Claim 1 is an independent claim to a document including, *inter alia*, plural bits of digital data steganographically in a graphic carried on the document. As noted, Nathans fails to teach this limitation.

In addition to not teaching any steganographic encoding, Nathans further fails to teach encoding plural bits of digital data in a graphic. The scrambling of the photo is accomplished by swapping pixels between locations in the image.[17] This is a one-way function: through use of a PIN a photo can be scrambled, but given a scrambled photo, the PIN cannot be derived. As such, Nathan's scrambled photo cannot be said to encode data (since the data cannot be decoded).

Still further, claim 1 specifies that text printed on the document and the steganographically encoded data cooperate to verify authenticity of the document. Nathans does not contemplate any cooperation between steganographically encoded data and printed text to as to verify authenticity of the document.

Accordingly, the anticipation rejection of claim 1 should be reversed.

Claim 4

Claim 4 depends from claim 1 and specifies that the digital data encoded in the graphic corresponds to at least part of the printed text on said document.

Nathan fails to teach such an arrangement.

Claim 5

Claim 5 depends from claim 1 and specifies that the digital data serves as an index into a registry containing additional information. (E.g., a passport photo can be steganographically encoded with a number that identifies a database record containing a dossier of information about the passport holder.)

Nathans fails to teach such an arrangement.

Claim 6

Claim 6 depends from claim 1 and belabors the obvious: the steganographic encoding does not visibly interrupt the graphic.

As noted, Nathans scrambles part of the photograph, visibly interrupting same.

Claim 8

Claim 8 depends from claim 1 and further specifies that "the printed text and the steganographically encoded plural bits of digital data cooperate to verify authenticity of the security document."

Again, Nathans includes no such teaching.

Claim 11

Claim 11 depends from claim 8 and specifies that the digital data encoded in the graphic corresponds to at least part of the printed text on said document.

As noted in connection with claim 4, Nathans provides no such teaching.

---

[17]   Nathans, col. 4, lines 11-19.

Claim 12

Claim 12 depends from claim 8 and specifies that the digital data serves as an index into a registry containing additional information.

As noted in connection with claim 5, Nathans fails to teach such an arrangement.

Claim 13

Claim 13 depends from claim 8 and again belabors the obvious: the steganographic encoding does not visibly interrupt the graphic.

As noted in connection with claim 6, Nathans scrambles part of the photograph, visibly interrupting same.

IX. CONCLUSION

The nonstatutory obviousness-type double-patenting rejections should be reversed as ill-founded. The claim rejections premised on Nathans should likewise be reversed because Nathans fails to teach the arrangements claimed.

Respectfully submitted,

DIGIMARC CORPORATION

Date: June 26, 2000

Digimarc Corporation
19801 SW 72nd Avenue, Suite 250   By
Tualatin, OR 97062   Joel R. Meyer
Phone: 503-885-8699   Registration No. 37,677

PENDING CLAIMS

1. A security document comprising:

a substrate;

text printed on the substrate;

a graphic carried by the substrate, the graphic conveying a visual impression to human viewers thereof;

the graphic additionally being steganographically encoded to secretly convey plural bits of digital data recoverable by computer analysis of said graphic.

2. The document of claim 1 in which the graphic is an image.

3. The document of claim 2 in which the image is a photographic image.

4. The document of claim 1 wherein said digital data corresponds to at least part of said printed text.

5. The document of claim 1 wherein said digital data serves as an index into a registry containing additional information.

6. The document of claim 1 wherein said steganographic encoding does not visibly interrupt said graphic.

7. The document of claim 1 wherein said steganographic encoding adds noise to the graphic, said noise not being perceptible as a representation of said plural-bit digital data except by computer analysis, wherein the encoded graphic does not appear to convey digital data to human viewers thereof.

8. The document of claim 1 in which the printed text and the steganographically encoded plural bits of digital data cooperate to verify authenticity of the security document.

9. The document of claim 8 in which the graphic is an image.

10. The document of claim 9 in which the image is a photographic image.

11. The document of claim 8 wherein said digital data corresponds to at least part of said printed text.

12. The document of claim 8 wherein said digital data serves as an index into a registry containing additional information.

13. The document of claim 8 wherein said steganographic encoding does not visibly interrupt said graphic.

14. The document of claim 8 wherein said steganographic encoding adds noise to the graphic, said noise not being perceptible as a representation of said plural-bit digital data except by computer analysis, wherein the encoded graphic does not appear to convey digital data to human viewers thereof.

15. An identity document according to claim 8.

16. An identity document according to claim 1.

17. A photo ID document comprising:

a photograph on a substrate, the photograph portraying an individual;

multi-bit information steganographically encoded within said photograph, said steganographic encoding not visibly interrupting the photograph;

wherein said encoding of the photograph serves to add noise thereto, but this noise is not perceptible as a representation of said multi-bit information except by computer analysis, wherein the encoded photograph appears to convey only an image of the individual to human viewers thereof.